USE OF ELECTRONIC COMMUNICATION TECHNOLOGY

I. PURPOSE

To provide employees with the use of up-to-date electronic communication technology in a way that is beneficial to the employee in his job, but not disruptive to the workplace.

II. SCOPE

This policy applies to all employees of the District.

III. POLICY

It is the policy of the District to place electronic communication technology in District facilities and to provide Internet and electronic mail access for use by employees in conducting District business.

IV. GUIDELINES

A. Computers are placed in all District facilities so that employees may complete their assigned duties and communicate with others outside of the District.

B. All components of this policy also apply to the use of all personal electronic technology devices, including but not limited to computers, Blackberries, iPhones, iPads, tablets, cell phones, watches, video recording devices, etc., that an employee may elect to bring onto District premises, as well as to any electronic communication devices that may be the property of the District.

C. The District utilizes both the Internet and an electronic mail system for business purposes. Additionally, while the District does provide electronic mail addresses for employees, the use of these systems is intended primarily for District-related work activities, as well as for those activities which promote skill building and knowledge enhancement. Employees shall limit the use of such systems for non-work related or personal business so that it does not interfere with daily operations.

D. It is the responsibility of each employee to ensure that District information disbursed via these systems is accurate, appropriate and lawful. Unauthorized copies of copyrighted or licensed materials on the Internet may not be created, distributed, or knowingly utilized.

E. Employees shall not expect privacy in their use of any electronic technology devices covered under this policy; management retains the right to review all employee activities on the systems.

F. Employees are to utilize only the software programs provided by the District on the District-owned computers or other electronic devices. Downloading of software programs to District computers or devices may only be done with the prior approval of the Fire Chief. Likewise, exporting system or other computer software is strictly prohibited without the prior approval of the Fire Chief.

G. While on duty or on District premises, employees are prohibited from accessing pornographic or otherwise inappropriate websites on the internet while on District premises. Social media websites such as Facebook, Myspace, Twitter, YouTube, etc., may be accessed for purposes of conducting District-related business. The use of such networking sites for purposes of general social communications shall be limited to down time and shall not interfere with the completion of one's duties. Additionally, any communications on such sites shall be subject to all of the guidelines set forth within this policy. Employee use of such sites shall be subject to monitoring and review. In addition, employee use of such sites while off-duty may come under scrutiny and review if the employee posts information on such websites that could reflect unfavorably upon the District, other employees or Board members, or the public we serve.

H. In using the electronic communications, employees shall not disclose any confidential information regarding the District, other employees, or the public we serve. Confidential information should be protected at all times. Employees should take all necessary steps to prevent unauthorized access to this information.

I. Employees shall use discretion in ensuring that their electronic communications reflect professional, respectful, and appropriate language and statements. The use of offensive language and/or disparaging remarks about the District or its employees or the public we serve shall not be tolerated.

J. Authorized users are responsible for the security of their individual passwords and accounts; passwords are not to be disclosed to others and should be changed quarterly.

K. All computers and remote devices should be secured with a password-protected screen saver and set to deactivate after being left unattended in excess of ten minutes.

L. Any introduction of malicious programs (i.e., viruses, worms) into the network or server is strictly forbidden and may result in disciplinary action up to and including termination.

M. Sending unsolicited e-mail messages (e-mail spam) to individuals who did not specifically request such or creating or forwarding chain letters or other “pyramid” type schemes shall be forbidden.

N. The posting to a website of any District-related photographs or electronic images taken on or off duty shall be at the sole discretion of the Fire Chief or his designee; employees shall obtain approval prior to such action.

O. Photographs or electronic images taken by an employee in the course of his employment are the sole property of the TFD and are under the control of the Fire Chief or his designated representative. This includes all images taken either intentionally or inadvertently by an employee with either a District owned or personally owned camera, cell phone, or other digital imaging device. TFD strictly prohibits the posting of any photographs or electronic images or media taken in the course of one’s employment on any personal website such as, but not limited to Facebook, Myspace, YouTube, etc. without prior approval from the Fire Chief.

P. Upon termination of employment with the District, employees are prohibited from taking, copying, or altering any computer-related programs, files, or materials for personal possession. Access to the District’s computer system shall be eliminated at the point of termination.